第３回会議の議論の整理（主なポイント）

資料１

１．セキュリティ・クリアランス制度へのニーズ、あるべき方向性

（１）国際的なビジネス・共同開発等でのニーズ

- 現状、日本における秘密情報の保持は、個々の契約ごと、あるいはプロジェクトごとに、契約により担保されている形になっている。資格要件となるベーシックな制度にはなっていないということが、１つの問題認識。Need to Know原則の下で、プロジェクトに必要な単位の人間で情報共有できるような仕組みとしてほしい。
- セキュリティ・クリアランス制度により、外国の政府との間での合意の下ではあるが、企業間での相互の情報共有が円滑になることが期待できる。実際、外国政府が保有する機微な情報についてのアクセスが得られず、日本から効果的な提案ができなかったことや、外国の企業が保有している機微な技術が得られないために、日本側で効果的な活用ができないなどの課題があった。
- こうした情報へのアクセスの質が向上することで、日本企業としてグローバルに経済安全保障分野に貢献することができ、成果物にかかるＱＣＤ（クオリティ、コスト、デリバリー）が向上するのではないか。
- また、様々なサイバーセキュリティ・インシデントが起きている中で、政府側が保有している様々な情報を開示してもらえれば、会社のセキュリティレベルの向上につながるだけではなく、新たなセキュリティ・テクノロジーの提案も可能となると考える。

（２）国際的な枠組み

- ファイブアイズに属する国家間において、どのような情報が共有されているかは明らかではないが、サイバーセキュリティに関する情報は広く共有されていると思われる。
- 日本とアメリカが一般的なＩＳＡ（Industrial Security Agreement；産業保全協定）を締結しても、ＩＳＡでアクセスできるのは、制度上、通常は極秘（Secret）まで。これ以上の機密（Top Secret）等にはアクセスできない。
- アメリカ政府が、機密（Top Secret）等の高い機微性をもつ情報まで、外国に親会社が存在するアメリカ子会社と共有することを認める決定がＮＩＤ（National Interest Determination；国益決定プロセス）であり、ＮＴＩＢ（National Technology Industrial Base;国家産業技術基盤）に加入している4か国（アメリカ、カナダ、オーストラリア、イギリス）は、ＮＩＤプロセスが免除される。

第３回会議の議論の整理（主なポイント）

１．セキュリティ・クリアランス制度へのニーズ、あるべき方向性

（３）日本とアメリカ等の違い・アメリカに通用する制度

- アメリカの制度を押さえておく意味は、アメリカから実質的に同等レベルの保護がなされているとみなされる制度を作ろうというのが共通認識であるため。いずれの企業からもそのような声があった。
- 日本でセキュリティ・クリアランス制度が出来れば、日本のセキュリティ・クリアランス保有者を増やしていく方向になる。海外と比べ、日本の方が事業規模に比して特定秘密保護法等のクリアランス保有者が少ない印象がある。
- アメリカでなぜセキュリティ・クリアランスが必要かの理由に、現実に外国政府等の工作員が活動している点を挙げてあるが、日本においても重要。
- セキュリティ・クリアランスには、人、施設及びサイバーセキュリティの３種類があるが、施設とサイバーセキュリティに関するセキュリティ・クリアランスの導入に反対する人は日本で多くないと思われる。議論となるのは人的セキュリティ・クリアランスであろう。その一つの要因には、日本と西洋の人間観の違いがある。我が国の社会は一般的に性善説に立っているため、ある人の人格等を悪あるいは弱さから把握しようとするセキュリティ・クリアランスは、その人の人格を全否定するような恐ろしい制度のように誤解される場合が多いのではないか。
- セキュリティ・クリアランスが取得できない場合に、当人が過去に何か悪いことや犯罪を行った人であるかのように捉えられがちであることを懸念。ただ、アメリカにおけるセキュリティ・クリアランスの判断基準を見ると、それはひとつの事象として見られているに過ぎず、むしろ外国の影響力がどのくらいあるのか、何か弱みがあってコントロールされてしまうのではないかといった観点で見られているという理解。
- アメリカのインテリジェンス機関や防衛産業で機微な情報を扱う仕事に従事する場合には、セキュリティ・クリアランスの保有と維持が雇用条件になっていることからセキュリティ・クリアランスを失うと解雇されることが多いのに対して、日本では労働者の解雇に対して非常に厳格なルールが存在していることから、セキュリティ・クリアランスが必要となる特定のプロジェクトの職務に就くことが予定されていた者が、セキュリティ・クリアランスを取得できなかった場合、そのこと自体は解雇事由にはならず、別のプロジェクト等に配転してもらうことが可能と思われる。
- 法令上の表現は異なっていても、基本的に各国とも、外国のインテリジェンス機関から付け込まれる人の弱さに関わる点に着目して、同様の判断を行っているものと考えられる。

第３回会議の議論の整理（主なポイント）

２．ニーズにこたえるための制度設計の方向性

（１）調査とプライバシー・従業員との関係

- 企業側で個人のバックグラウンドを調べるのは難しいという印象。どういう項目をどう調べるのかは政府側で決めていただきたい。
- セキュリティ・クリアランス取得が求められる国家安全保障に直結する職務は世の中のうちほんの僅か。当該職に就けなくても生活に困ることは稀であろう。
- 諸外国との実質的同等性を確保するとともに、経済活動を阻害しないこと、また日本においての労働法制との調和も課題。

（２）ＣＵＩ

- アメリカが全ての機微な技術をＣＩとして指定することができないのは、自国でこれらの技術を用いた製品を全て製造することはできず、日本の精密技術なども利用する必要があるため。したがって、このような技術の多くはＣＵＩに指定されている。
- 特に半導体分野がそうであるが、アメリカが重要技術として指定した技術に対しては、今後も規制は強化されることが予想されることから、それに関連するＣＩやＣＵＩの範囲も拡大していくものと思われる。
- 現在、アメリカでは、ＣＵＩに関する統一的な身上調査規定は存在していないものと思われ、その人的スクリーニング（バックグラウンド・チェック）は、個別の制度ごとに設定されているものと考えられる。
- ＣＵＩに該当する部分について、特に民間企業においてどういった形で規律していくのかということについて、土俵となるのは不正競争防止法以外ないのではないか。

第３回会議の議論の整理（主なポイント）

２．ニーズにこたえるための制度設計の方向性

（３）大学・研究機関

- アメリカでは、大学や研究機関が国家の機密情報を扱う場合、連邦政府が所有・運営している組織の場合には連邦行政機関と同じセキュリティ・クリアランス制度が適用され、民間が運営する組織の場合には、民間の請負人に適用される国家産業保全プログラムにおけるセキュリティ・クリアランスが必要になる。
- 他方、アメリカにおける大学へのセキュリティ・クリアランスと同様の制度を、日本の大学にそのまま適用することはできないと考える。現在、一般の大学に所属し、将来的にセキュリティ・クリアランスが必要となる情報に接することに同意していただける研究者の方は、現状では、法人に対してセキュリティ・クリアランスを実施することができる国立の研究機関や民間企業に移っていただくしかないと考えられる。
- 移籍していただく研究者の方には、報酬、研究費、必要となる施設などの面で十分に処遇する必要がある。研究機関については、アメリカにおいてもリサーチ・インテグリティをいかに保全していくかが大きな課題となっており、かつこの点が一番弱いと言ってもいい。この辺りを我が国でどのように対応していくかは大きな課題。

（４）その他

- アメリカでは、民間事業者に対するセキュリティ・クリアランス制度が、政府関係とは別にあるということは、経済安全保障の世界の中でセキュリティ・クリアランスを位置づけられることを考えられるものであり、とても示唆に富んだ制度であると思う。
- セキュリティ・クリアランス制度が事務局資料２（諸外国制度比較）のどこの国にもあるということは分かったが、クリアランス保持者は何人いるのか、これが実際に定着して実態的な運用が行われているということについても追加的な情報をいただければ、世界では非常に普及している制度であるが、日本だけができていないということが分かる。
- 今後クリアランスの調査項目の比較も、各国制度との同等性の観点を検討する上で重要だと思う。